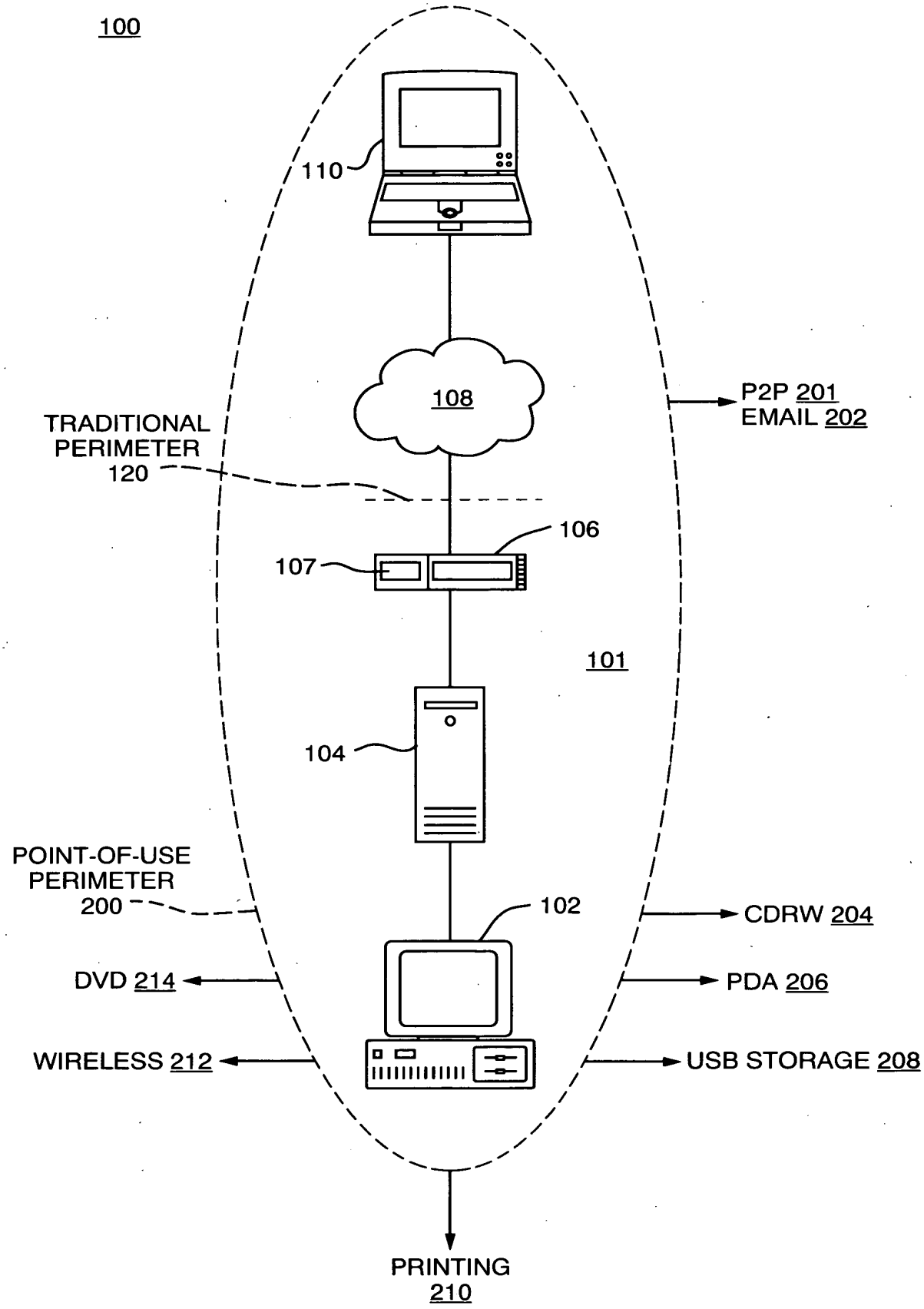


FIG. 1

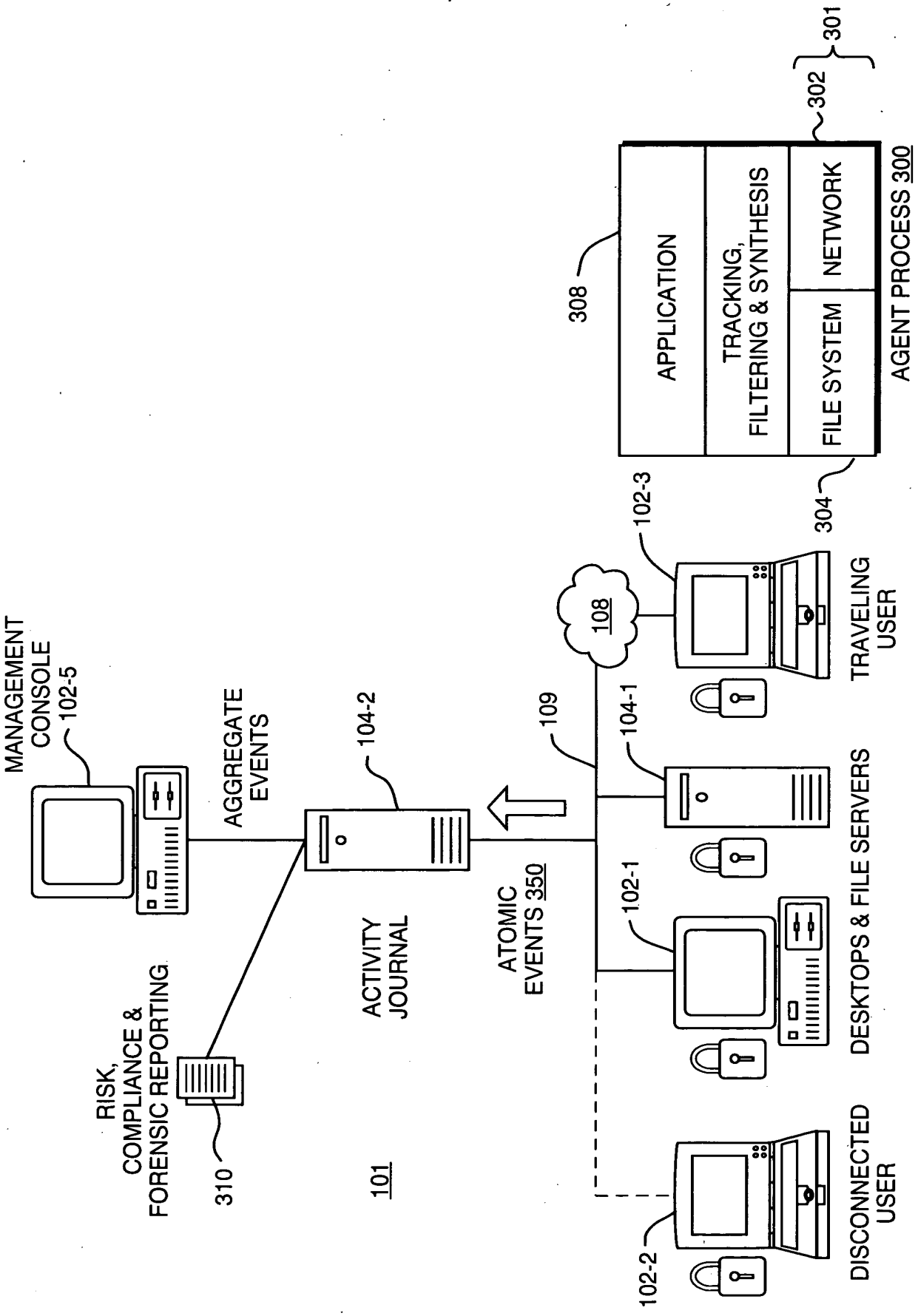

301
302
APPLICATION
TRACKING, FILTERING & SYNTHESIS
NETWORK
FILE SYSTEM
AGENT PROCESS 300
308
304
102-3
TRAVELING USER
108
109
104-1
DESKTOPS & FILE SERVERS
102-1
DISCONNECTED USER
102-2
ATOMIC EVENTS 350
ACTIVITY JOURNAL
104-2
AGGREGATE EVENTS
MANAGEMENT CONSOLE
102-5
RISK, COMPLIANCE & FORENSIC REPORTING
310
101

FIG. 2

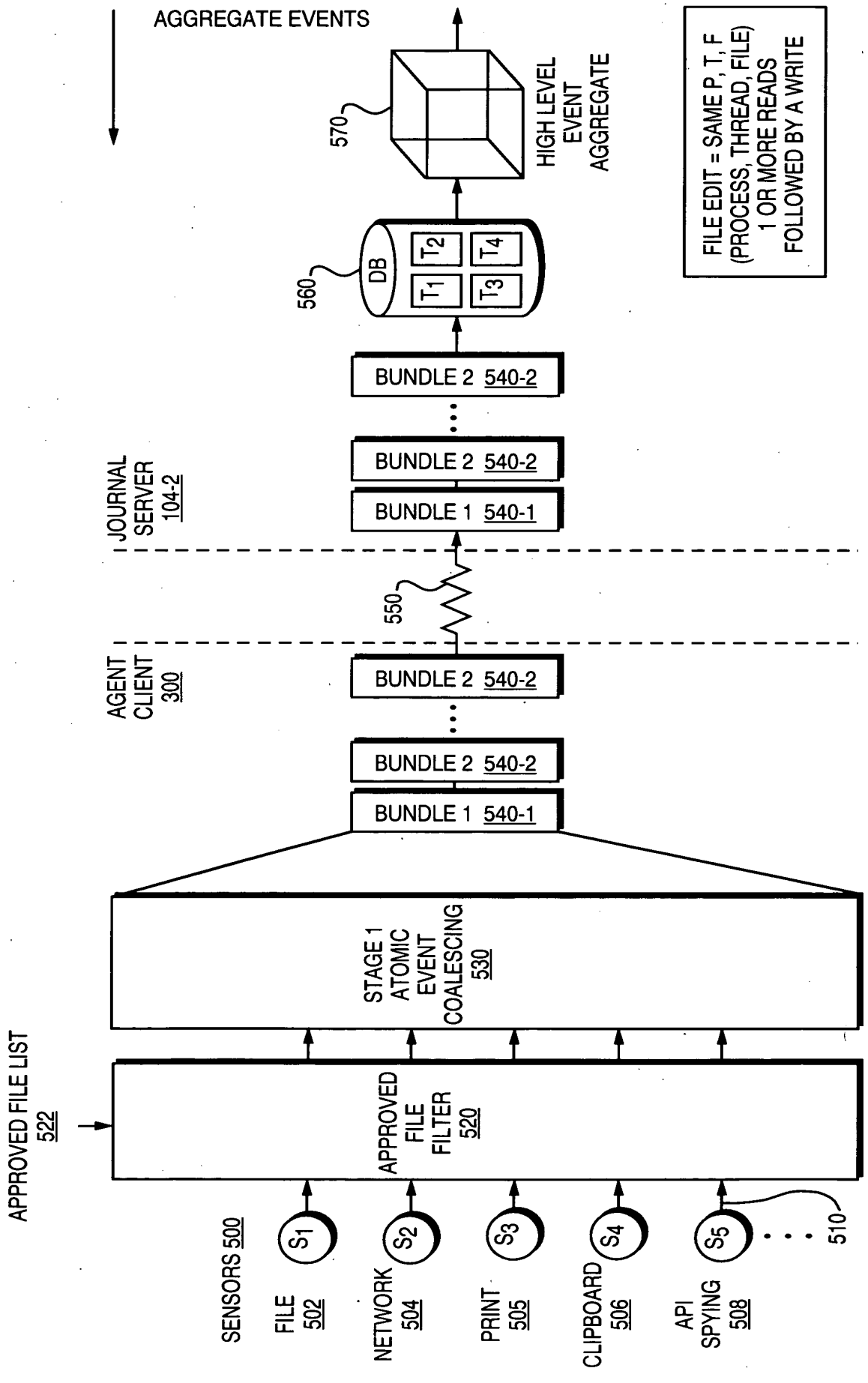

AGGREGATE EVENTS
570
HIGH LEVEL EVENT AGGREGATE
FILE EDIT = SAME P, T, F (PROCESS, THREAD, FILE) 1 OR MORE READS FOLLOWED BY A WRITE
560
DB
T1
T2
T3
T4
BUNDLE 2 540-2
BUNDLE 2 540-2
BUNDLE 1 540-1
JOURNAL SERVER 104-2
550
AGENT CLIENT 300
BUNDLE 2 540-2
BUNDLE 2 540-2
BUNDLE 1 540-1
STAGE 1 ATOMIC EVENT COALESCING 530
APPROVED FILE LIST 522
APPROVED FILE FILTER 520
95%
SENSORS 500
S1
S2
S3
S4
S5
510
FILE 502
NETWORK 504
PRINT 505
CLIPBOARD 506
API SPYING 508

FIG. 3

Action Type	Level	Event Category	Event Name	Event Table	Action Detail Field	Action Detail Value	Discriminant
1	Low	File	FileRead	FileEvent	operationType	0	bytesRead > 0, bytesWritten = 0
2	Low	File	FileWnte	FileEvent	operationType	0	bytesRead = 0, bytesWritten > 0
3	Low	File	FileReadWrite	FileEvent	operationType	0	bytesRead > 0, bytesWritten > 0
4	Low	File	FileCopy	FileEvent	operationType	1	
5	Low	File	FileRename	FileEvent	operationType	2	
6	Low	File	FileDelete	FileEvent	operationType	3	
7	Low	File	FileMove	FileEvent	operationType	4	
8	Low	File	FileRecycle	FileEvent	operationType	5	
9	Low	File	FileRestore	FileEvent	operationType	6	
10	Low	Network	TCPIPInbound	NetworkEvent	protocolType	TCPIP	isOutbound = 0
11	Low	Network	TCPIPOutbound	NetworkEvent	protocolType	TCPIP	isOutbound = 1
12	Low	Network	UDPInbound	NetworkEvent	protocolType	UDP	isOutbound = 0
13	Low	Network	UDPOutbound	NetworkEvent	protocolType	UDP	isOutbound = 1
14	Low	Network	IPSECInbound	NetworkEvent	protocolType	IPSEC	isOutbound = 0
15	Low	Network	IPSECOutbound	NetworkEvent	protocolType	IPSEC	isOutbound = 1
16	Low	Print	Print	PrintEvent	(implied)	N/A	
17	Low	CD	CDRead	CDEvent	operationType	1	
18	Low	CD	CDWrite	CDEvent	operationType	2	
19	Low	Clipboard	ClipboardCutCopy	ClipboardEvent	eventType	CutCopy	
20	Low	Clipboard	ClipboardPaste	ClipboardEvent	eventType	Paste	
21	Low	User	UserLogon	UserEvent	eventType	Logon	
22	Low	User	UserLogoff	UserEvent	eventType	Logoff	
23	Low	Machine	Machine	MachineEvent	eventType	• • •	Skip the Machine events

FIG. 4A

24	Low	Process	ProcessStart	Process	(Implied)		Use processStartDtTm	
25	Low	Process	ProcessEnd	Process	(Implied)		Use processEndDtTime	
26	High	File	FileEdited	AggregateEvent				
27	High	File	FileCopied	AggregateEvent				
28	High	File	FileSaveAs	AggregateEvent				
29	High	File	FileLeftThroughRemovableMedia	AggregateEvent				
30	High	Clipboard	ClipboardToFile	AggregateEvent				
31	High	Print	PrintFile	AggregateEvent				
32	High	CD	BurnMaster	AggregateEvent				
33	High	CD	BurnFile	AggregateEvent				
34	High	Network	FileLeftThroughNetworkPort	AggregateEvent				
35	High	Network	EmailFile	AggregateEvent				
36	High	Network	RemoteAccess	AggregateEvent				
37	High	Network	InstantMessenger	AggregateEvent				
38	High	Network	P2PApp	AggregateEvent				
39	High	Network	FTPFile	AggregateEvent				
40	High	Network	TunnelOut	AggregateEvent				
41	High	Network	TunnelIn	AggregateEvent				
42	High	Network	TunnelInOut	AggregateEvent				
43	High	Network	FileOutThroughTunnel	AggregateEvent				

FIG. 4B

Event Name	Constituent Event Types	Pattern	Scope
FileEdited	FileRead, FileWrite, FileReadWrite	Same processid and fileHandle. beforeHash of first read & afterHash of last write differ. Both reads and writes to same fileHandle. Sum of writes > 0.	Thread
FileCopied	FileRead, FileWrite, FileReadWrite, FileCopy	Command shell: Alternating reads & writes. The reads all have one filehandle, the writes all have a second one. Explorer: A long series of reads from one filehandle followed by a long series of writes to a second. Miind the time period between. In both cases, the target device must not be removable.	Thread
FileSaveAs	FileRead, FileWrite, FileReadWrite	An app reads one or more files then writes a file.	Process
FileLeftThroughRemovableMedia	FileRead, FileWrite, FileReadWrite, FileCopy	Same as FileCopied or FileSaveAs, but target device is removable.	Process
ClipboardToFile	ClipboardCutCopy, ClipboardPaste	Pair a ClipboardCutCopy with all subsequent Clipboard Paste events for that user login until the next copy or the user logs out. Problem: If the user closes the application that performed the copy and the object was large and the user opts not to keep it there, what happens ?	Login

FIG. 5A

PrintFile	Print, possibly others	Unclear. If there are temp files, intermediate PDF files, etc. then we may perform a chain of custody analysis to figure out just what was printed.	Thread
BurnMaster	FileRead, FileWrite	An app known to burn files reads one or more files then writes a file.	Process
BurnFile	CDWrite, FileRead	Application is recognized as a CD writing app. (Optional) Series of FileReads from one fileHandle, followed by a series of CDWrite events with the same process. May need to compare filenames, otherwise one read will exhaust all the writes. Alternately, all read files are lumped together with one large burn event. Or perhaps the first read of a new file after the last read from the previous file is the start of the next burn event.	Process
FileLeftThroughNetworkPort	FileRead, TCPIPInbound, TCPIPOutbound, UDPInbound, UDPOutbound, IPSECInbound, IPSECOutbound	An overlapping stream of FileReads interspersed with Inbound and Outbound network events. All the network events should be for the same port (?) and to a destination NOT on localhost. All the network events should be for the same protocol.	Thread
EMailFile	FileRead, TCPIPInbound, TCPIPOutbound, (other protocols???)	Similar to FileLeftThroughNetworkPort. Combines all interleaving FileReads with the network events. The application image name is one of those known to be an email program. May place constraints on the ports, since many emailers use certain well defined ports for SMTP, POP, etc.	Process

FIG. 5B

InstantMessenger	FileRead, TCPIPInbound, TCPIPOutbound, (other protocols???)	Similar to FileLeftThroughNetworkPort. Combines all interleaving FileReads with the network events. The application image name is one of those known to be used for instant Messanger. May place constraints on the ports.	Process
P2PApp	FileRead, TCPIPInbound, TCPIPOutbound, UDPInbound, UDPOutbound, IPSECInbound, IPSECOutbound	Constrain the application name to be one of those known to be a P2PApp. Multiple ports will be used; some or all of them may have constraints. May constrain the protocol per app or per instance. Similar to FileLeftThroughNetworkPort as concerns interleaved file reads.	Process
FTPFile	FileRead, FileWrite, ??? (TCPIPInbound, TCPIPOutbound	May want to split into two events, one for reading and one for writing. Constrain to the common FTP port, unless the app is known by name to be an FTP client. Like FileLeftThroughNetworkPort, look for interleaved reads and network events, or interleaved writes and network events.	Process
RemoteAccess	TCPIPInbound, TCPIPOutbound, UDPInbound, UDPOutbound, IPSECInbound, IPSECOutbound	Do not incorporate FileRead events. Several ports may be used. Look for known image names of remote apps.	Process

FIG. 5C

TunnelOut	TCPIPInbound, TCPIPOutbound, UDPInbound, UDPOutbound, IPSECInbound, IPSECOutbound	All events use same protocol. Only two processes used. Two different apps and four ports are used. One of the ports is remote. Event 1: The first app sends outbound from local port 1 to local port 2. Event 2: The second app (the tunneler) receives inbound from local port 1 to local port 2. Event 3: The tunneler also sends from local port 3 to remote port 4. Both events of the tunneler share the same thread (probably).	Login
TunnelIn	TCPIPInbound, TCPIPOutbound, UDPInbound, UDPOutbound, IPSECInbound, IPSECOutbound	All events use same protocol. Only two processes used. Two different apps and four ports are used. one of the ports is remote. Event 1: The first app (the tunneler) receives inbound from remote port 1 to local port 2. Event 2: The tunneler sends outbound from local port 2 to local port 3. Event 3: The second app also receives inbound from local port 3 to local port 4. Both events of the tunneler share the same thread (probably).	Login
TunnelInOut	TCPIPInbound, TCPIPOutbound, UDPInbound, UDPOutbound, IPSECInbound, IPSECOutbound	Multiple protocols may be used. More research needed. More than three ports are used.	Login
FileLeftThroughTunnel	FileRead, TunnelOut	Similar to FileLeftThroughNetworkPort. Combines all interleaving FileReads involving a process that is participating in a TunnelOut event. If more than one file is read, the source destination will be a count of the files read.	Login?

FIG. 5D

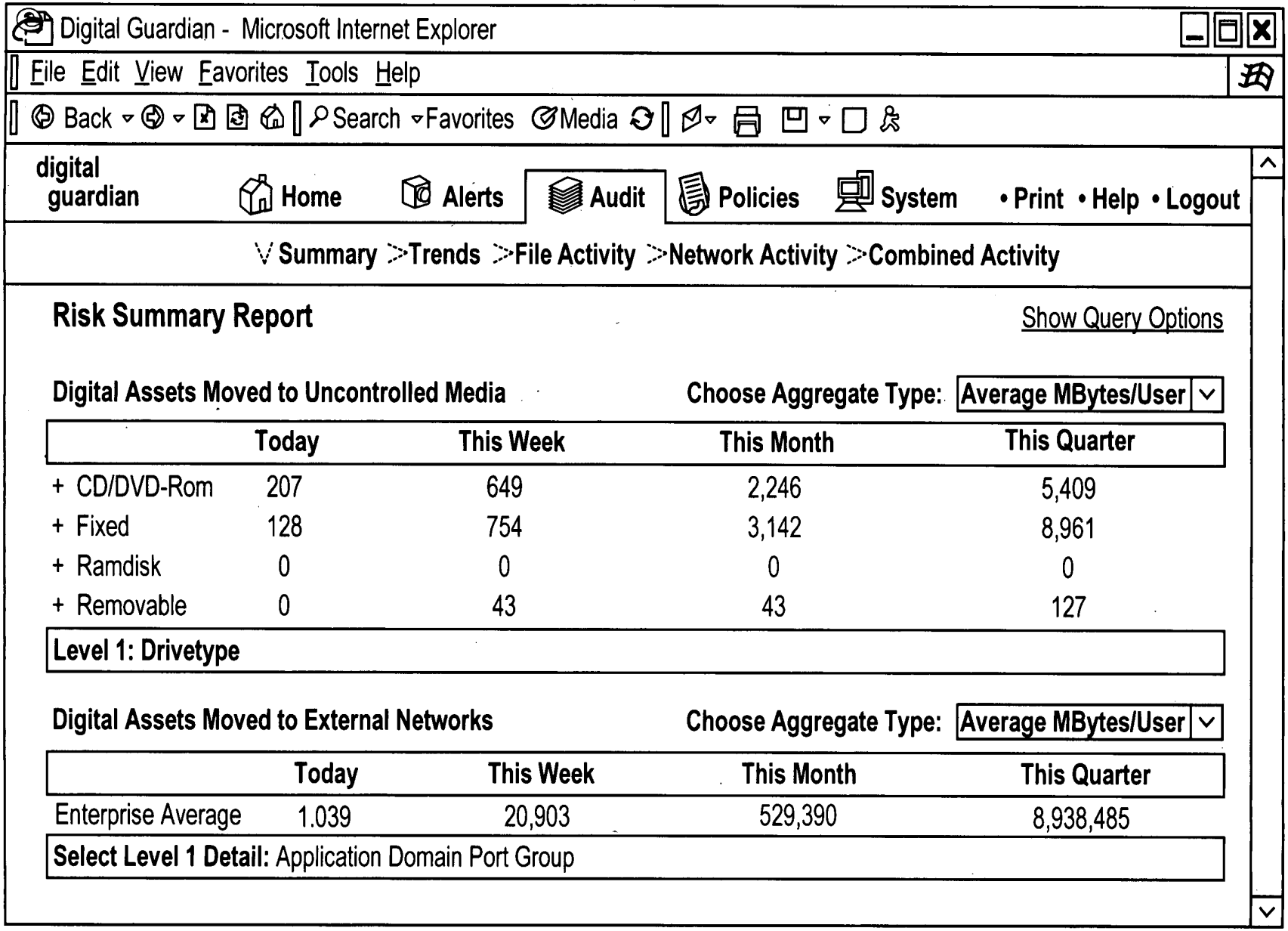
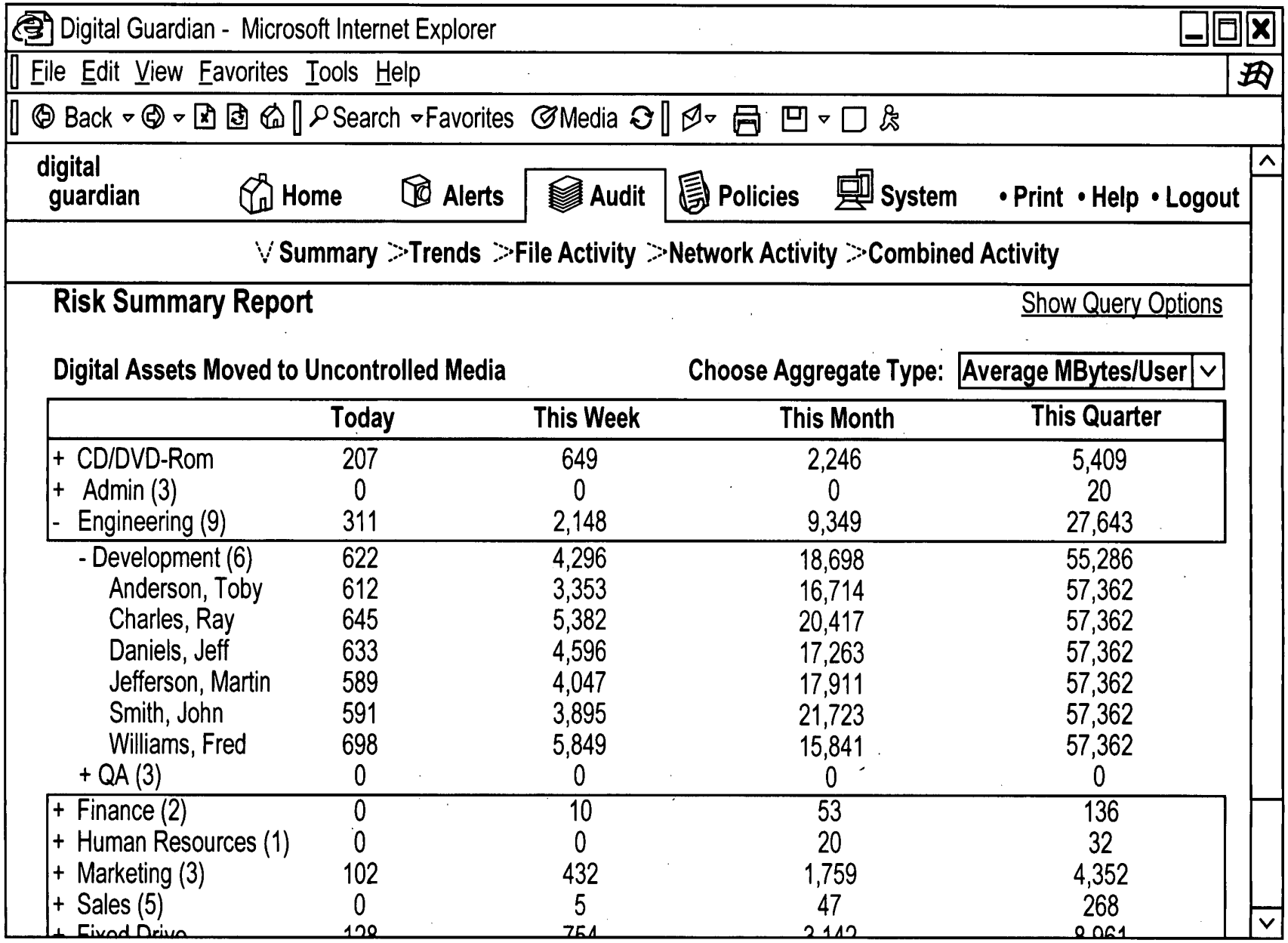

Digital Guardian - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
digital guardian
Home
Alerts
Audit
Policies
System
• Print • Help • Logout
Summary >Trends >File Activity >Network Activity >Combined Activity
Risk Summary Report
Show Query Options
Digital Assets Moved to Uncontrolled Media
Choose Aggregate Type: Average MBytes/User
Today This Week This Month This Quarter
+ CD/DVD-Rom 207 649 2,246 5,409
+ Fixed 128 754 3,142 8,961
+ Ramdisk 0 0 0 0
+ Removable 0 43 43 127
Level 1: Drivetype
Digital Assets Moved to External Networks
Choose Aggregate Type: Average MBytes/User
Today This Week This Month This Quarter
Enterprise Average 1.039 20,903 529,390 8,938,485
Select Level 1 Detail: Application Domain Port Group

FIG. 6A



	Today	This Week	This Month	This Quarter
+ CD/DVD-Rom	207	649	2,246	5,409
+ Admin (3)	0	0	0	20
- Engineering (9)	311	2,148	9,349	27,643
- Development (6)	622	4,296	18,698	55,286
Anderson, Toby	612	3,353	16,714	57,362
Charles, Ray	645	5,382	20,417	57,362
Daniels, Jeff	633	4,596	17,263	57,362
Jefferson, Martin	589	4,047	17,911	57,362
Smith, John	591	3,895	21,723	57,362
Williams, Fred	698	5,849	15,841	57,362
+ QA (3)	0	0	0	0
+ Finance (2)	0	10	53	136
+ Human Resources (1)	0	0	20	32
+ Marketing (3)	102	432	1,759	4,352
+ Sales (5)	0	5	47	268
+ Fixed Drive	128	754	2,142	8,061

FIG. 6B

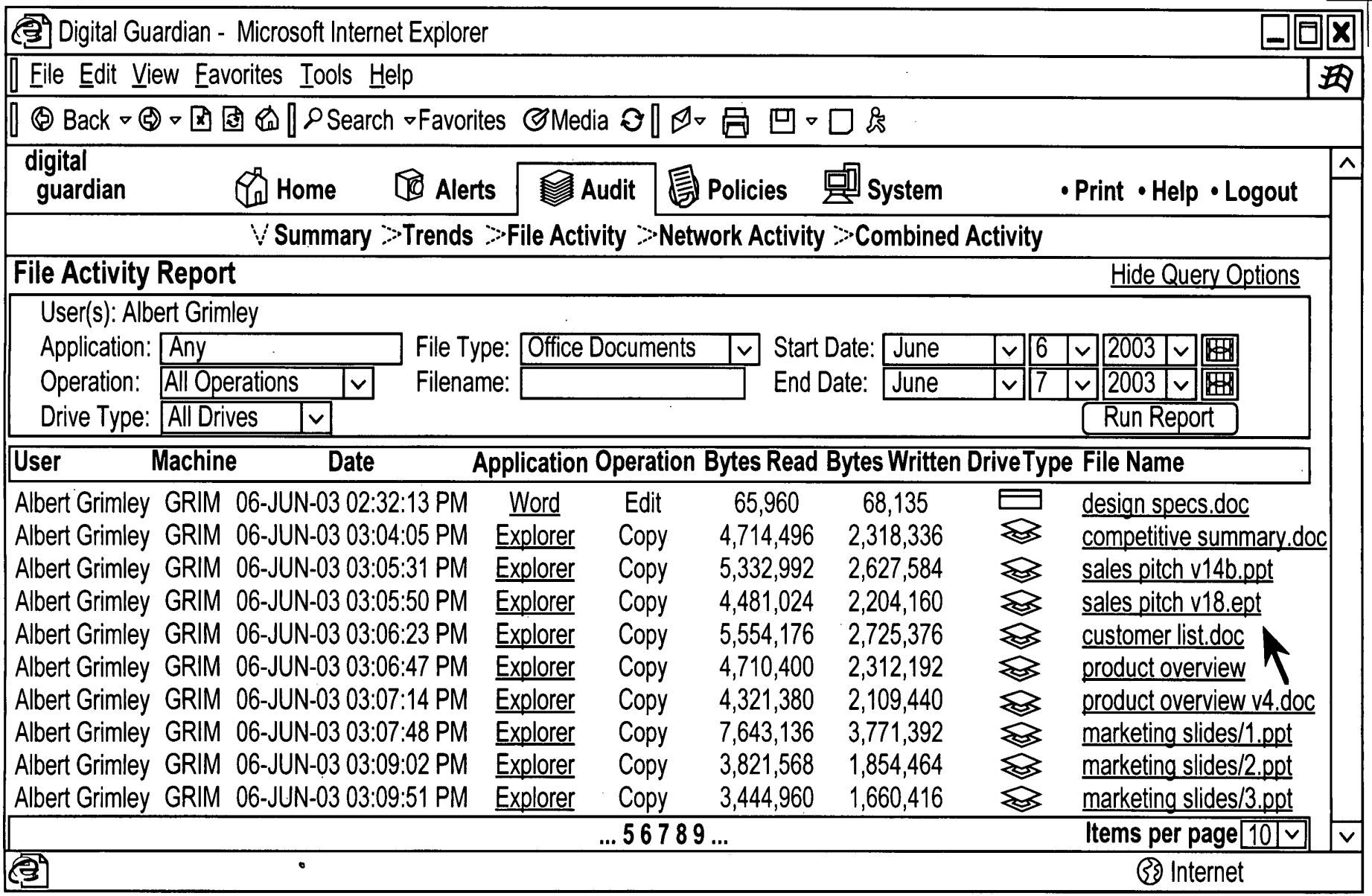

Digital Guardian - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
digital guardian
Home
Alerts
Audit
Policies
System
• Print • Help • Logout
Summary >Trends >File Activity >Network Activity >Combined Activity
File Activity Report
Hide Query Options
User(s): Albert Grimley
Application: Any
File Type: Office Documents
Start Date: June 6 2003
Operation: All Operations
Filename:
End Date: June 7 2003
Drive Type: All Drives
Run Report
User Machine Date Application Operation Bytes Read Bytes Written Drive Type File Name
Albert Grimley GRIM 06-JUN-03 02:32:13 PM Word Edit 65,960 68,135 design specs.doc
Albert Grimley GRIM 06-JUN-03 03:04:05 PM Explorer Copy 4,714,496 2,318,336 competitive summary.doc
Albert Grimley GRIM 06-JUN-03 03:05:31 PM Explorer Copy 5,332,992 2,627,584 sales pitch v14b.ppt
Albert Grimley GRIM 06-JUN-03 03:05:50 PM Explorer Copy 4,481,024 2,204,160 sales pitch v18.ept
Albert Grimley GRIM 06-JUN-03 03:06:23 PM Explorer Copy 5,554,176 2,725,376 customer list.doc
Albert Grimley GRIM 06-JUN-03 03:06:47 PM Explorer Copy 4,710,400 2,312,192 product overview
Albert Grimley GRIM 06-JUN-03 03:07:14 PM Explorer Copy 4,321,380 2,109,440 product overview v4.doc
Albert Grimley GRIM 06-JUN-03 03:07:48 PM Explorer Copy 7,643,136 3,771,392 marketing slides/1.ppt
Albert Grimley GRIM 06-JUN-03 03:09:02 PM Explorer Copy 3,821,568 1,854,464 marketing slides/2.ppt
Albert Grimley GRIM 06-JUN-03 03:09:51 PM Explorer Copy 3,444,960 1,660,416 marketing slides/3.ppt
... 5 6 7 8 9 ...
Items per page 10
Internet

FIG. 6C